(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年5 月13 日 (13.05.2004)

PCT

(10) 国際公開番号
WO 2004/040838 A1

(51) 国際特許分類[7]: H04L 9/24, G06F 7/58

(21) 国際出願番号: PCT/JP2003/014055

(22) 国際出願日: 2003 年11 月4 日 (04.11.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-320035 2002 年11 月1 日 (01.11.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO.,LTD.) [JP/JP]; 〒570-8677 大阪府 守口市京阪本通 2丁目5番5号 Osaka (JP). 株式会社数理設計研究所 (KABUSHIKI KAISHA SURI SEKKEI KENKYUSHO) [JP/JP]; 〒371-0816 群馬県 前橋市上佐鳥町 54−2 Gunma (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 女屋 正人 (ONAYA,Masato) [JP/JP]; 〒570-8677 大阪府 守口市京阪本通 2丁目5番5号 三洋電機株式会社内 Osaka (JP). 玉置 晴朗 (TAMAKI,Haruro) [JP/JP]; 〒371-0816 群馬県 前橋市上佐鳥町 54−2 株式会社数理設計研究所内 Gunma (JP). 池谷 昭 (IKETANI,Akira) [JP/JP]; 〒110-0005 東京都 台東区上野 1丁目19番10号 三洋セミコンデバイス株式会社内 Tokyo (JP).

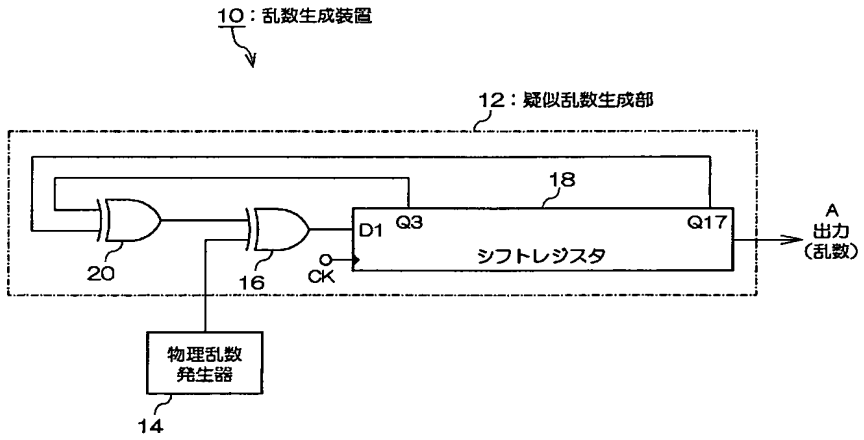
(74) 代理人: 吉田 研二, 外 (YOSHIDA,Kenji et al.); 〒180-0004 東京都 武蔵野市吉祥寺本町 1丁目34番12号 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

[続葉有]

(54) Title: RANDOM NUMBER GENERATION DEVICE

(54) 発明の名称: 乱数生成装置



10...RANDOM NUMBER GENERATION DEVICE
12...PSEUDO RANDOM NUMBER GENERATION SECTION
18...SHIFT REGISTER
14...PHYSICAL RANDOM NUMBER GENERATION SECTION
A...OUTPUT (RANDOM NUMBER)

(57) Abstract: A random number generation device includes a pseudo random number generation section capable of outputting a plurality of random numbers of different pseudo random number series, a physical random number generation section for generating a physical random number, and a switching section for switching the pseudo random number series of the random numbers output from the pseudo random number generation section according to the physical random number generated by the physical random number generation section. The output of the pseudo random number generation section is used as an output random number. Since a plurality of different pseudo random number series are switched to be output by a physical random number, it is possible to reduce the predictability of the random number as compared to the conventional random number generation device using only a pseudo random number. Moreover, since the physical random number is not directly used as an output random number, even if any operation is added to the physical random number generation means from outside, the affect for the predictability of the output random number is significantly lowered as compared to the conventional device.

[続葉有]

WO 2004/040838 A1

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 乱数生成装置は、複数の異なる疑似乱数系列の乱数を出力可能な疑似乱数生成部と、物理乱数を生成する物理乱数発生器と、物理乱数発生器の生成した物理乱数に基づいて疑似乱数生成部の出力する乱数の疑似乱数系列を切り替える切替部と、を備え、疑似乱数生成部の出力を出力乱数とする。複数の異なる疑似乱数系列を物理乱数によって切り替えて出力するため、従来の疑似乱数のみを用いた乱数生成装置に比べて乱数の予測性を低減することができる。また、物理乱数を直接的な出力乱数としては用いないため、仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測性に対する影響は従来装置に比べてかなり小さくなる。

明　細　書

乱数生成装置

技術分野

本発明は、乱数生成装置に関し、特に暗号化アルゴリズムに好適な乱数生成装置に関する。

背景技術

暗号化アルゴリズム等では、セキュリティの確保のために、しばしば乱数が用いられる。その場合の乱数としては、一般的に、M系列（Maximum length code：最長符号系列）等に代表される疑似乱数が用いられてきた。M系列符号は、公知の線形シフトレジスタ符号発生器によって生成することができる。

また、上記疑似乱数以外の乱数として、原子核の崩壊現象がランダムとなることや電気雑音等の自然現象を利用して生成される物理乱数が知られている。暗号化アルゴリズム等においても、上記疑似乱数に替えて、この物理乱数を利用する場合もある（例えば、日本特開２０００－６６５９２公報参照。）

しかしながら、M系列等に代表される疑似乱数は、必ずしも安全性の高い乱数とは言えず、セキュリティ確保の面からは好ましくないところがある。疑似乱数は、一定の算術プロセスあるいは関数の組み合わせから生成されるため、同じ初期条件を与えれば同一の値となり、乱数の推定が可能となるからである。

また、一般的に物理乱数は微弱な信号であるため、暗号化アルゴリズム等で使用するためには、通常、増幅器によって利用可能なレベルに増幅される。ところが、これら全体は電界や磁界によって影響を受ける場合があり、それらの意図的または意図せざる印加によって乱数の発生確率が操作され、安全性が低下してしまう場合があった。

発明の開示

本発明にかかる乱数生成装置は、複数の異なる疑似乱数系列の乱数パターンを

出力可能な疑似乱数生成手段と、物理乱数を生成する物理乱数生成手段と、上記物理乱数生成手段の生成した物理乱数に基づいて上記疑似乱数生成手段の出力する乱数の疑似乱数系列を切り替える切替手段と、を備える。すなわち、上記本発明にかかる乱数生成装置によれば、複数の異なる疑似乱数を物理乱数によって切り替えて出力するため、従来の疑似乱数のみを用いた乱数生成装置に比べて乱数の予測性を低減することができる。また、物理乱数を直接的な出力乱数としては用いていないため、仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測性に対する影響は従来装置に比べてかなり小さくなる。

上記本発明にかかる乱数生成装置は、種々の形態によって実現することができる。例えば、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段が、線形シフトレジスタ符号発生器を含み、上記切替手段が、上記線形シフトレジスタ符号発生器への帰還入力値の反転／非反転を、上記物理乱数生成手段によって生成された物理乱数に基づいて切り替えるよう、構成することができる。

また、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、上記切替手段は、上記線形シフトレジスタ符号発生器からの出力値の反転／非反転を、上記物理乱数生成手段によって生成された物理乱数に基づいて切り替えるよう、構成することができる。

また、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段が、線形シフトレジスタ符号発生器を含み、該線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく複数の帰還入力値を生成し、上記切替手段が、上記生成された複数の帰還入力値のうち該線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、上記物理乱数生成手段で生成された物理乱数に基づいて切り替えるよう、構成することができる。

また、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段が、所定のタップの組み合わせに基づく第一の帰還入力値を生成する線形シフトレジスタ符号発生器と、該第一の帰還入力値を受け取り上記線形シフトレジスタ符号発生器と同期して所定ビット数ビットシフトを行いその出力を第二の帰還入力値とするフリップフロップと、を含み、上記切替手段が、上記第一または第二の帰還入力値のうち上記線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、上記

物理乱数生成手段で生成された物理乱数に基づいて切り替えるよう、構成することができる。

また、上記本発明にかかる乱数生成装置では、上記線形シフトレジスタ符号発生器の符号列を検出する検出手段を備え、上記切替手段は、有効なまたは切り替えによって有効となる疑似乱数系列の乱数が上記検出された符号列によっては生成不能である場合には、該疑似乱数系列以外の疑似乱数系列に切り替えるのが好適である。これにより、線形シフトレジスタ符号発生器において有効な疑似乱数系列に対して疑似乱数の生成されない符号列となるのが抑制される。

また、上記本発明にかかる乱数生成装置では、上記線形シフトレジスタ符号発生器の符号列を検出する検出手段と、有効なまたは切り替えによって有効となる疑似乱数系列の乱数が上記検出された符号列によっては生成不能である場合には、上記符号列のビット値のうち少なくとも一つを反転させるのが好適である。このような構成によっても、線形シフトレジスタ符号発生器において有効な疑似乱数系列に対して疑似乱数の生成されない符号列となるのが抑制される。

図面の簡単な説明

図１は、本発明の実施の形態１にかかる乱数生成装置の構成図である。

図２は、本発明の実施の形態１にかかる乱数生成装置によって生成される疑似乱数系列の一例を示す図である。

図３は、本発明の実施の形態にかかる物理乱数発生器の構成図である。

図４は、本発明の実施の形態２にかかる乱数生成装置の構成図である。

図５は、本発明の実施の形態３にかかる乱数生成装置の構成図である。

図６は、本発明の実施の形態３にかかる乱数生成装置によって生成される疑似乱数系列の一例を示す図である。

図７は、本発明の実施の形態４にかかる乱数生成装置の構成図である。

図８は、本発明の実施の形態４にかかる乱数生成装置によって生成される疑似乱数系列の一例を示す図である。

図９は、本発明の実施の形態５にかかる乱数生成装置の構成図である。

図１０は、本発明の実施の形態５にかかる乱数生成装置によって生成される疑

似乱数系列の一例を示す図である。

図１１は、本発明の実施の形態６にかかる乱数生成装置の構成図である。

発明を実施するための最良の形態

実施の形態１．　図１は本実施形態にかかる乱数生成装置１０の構成図、図２は乱数生成装置１０によって生成される二つのM系列の巡回パターンを示す図、また図３は物理乱数発生器１４の構成図である。

乱数生成装置１０は、疑似乱数生成部１２、物理乱数発生器１４、および切替部１６を含む。このうち疑似乱数生成部１２は、少なくとも一つの線形シフトレジスタ符号発生器を含み、複数の異なる疑似乱数系列（例えば、M系列等）の乱数パターンを出力することができる。本実施形態では、縦続して接続された複数のフリップフロップを含むシフトレジスタ１８と、所定の複数のタップ位置からの出力値の排他的論理和を出力するＥＸＯＲゲート２０と、が設けられており、これらにより、M系列の乱数を出力する線形シフトレジスタ符号発生器が構成されている。図１の例では、シフトレジスタ１８は、１７個のフリップフロップを有しクロック（ＣＫ）に応じてビットシフトする１７段シフトレジスタとして構成され、入力側より第３番目と第１７番目のフリップフロップからのタップ出力（Q出力；Ｑ３，Ｑ１７）に基づいて帰還入力値（シフトレジスタ１８のＤ１入力；「１」（ハイレベル）または「０」（ローレベル））が生成される。

一般的な線形シフトレジスタ符号発生器では、ＥＸＯＲゲート２０の出力がそのままシフトレジスタ１８に帰還入力されるが、本実施形態では、ＥＸＯＲゲート２０の出力は切替部１６を経由してシフトレジスタ１８に入力される。切替部１６は、物理乱数発生器１４からの物理乱数出力（バイナリコード）に基づいて、帰還入力値となるＥＸＯＲゲート２０からの出力値の反転／非反転を切り替える。すなわち、この物理乱数出力は、切替制御信号と言うことができる。図１の例では、切替部１６は、ＥＸＯＲゲートとして構成される。ＥＸＯＲゲートは、二つの入力値が不一致であるときに「１」を出力し、一致するときに「０」を出力する。したがって、物理乱数出力値が「１」であるときは、切替部１６においてＥＸＯＲゲート２０の出力値は反転され、他方、物理乱数出力値が「０」であると

きは、反転されない。つまり、切替部１６は、物理乱数出力値に応じて、ＥＸＯＲゲート２０からの出力値を反転して帰還入力値とするか、あるいは反転させずにそのまま帰還入力値とするかを、切り替えていることになる。

このような切替部１６の動作により、疑似乱数生成部１２は、異なる二つの疑似乱数系列を生成することができる。図１の例では、物理乱数出力値が「０」であるときは切替部１６において帰還入力値は反転されないから、疑似乱数生成部１２においてクロック信号（ＣＫ）に基づいて 2^{17}-1 サイクルで循環的に変化するＭ系列１－１（図２（ａ））が生成され、他方、物理乱数出力値が「１」であるときは、切替部１６において帰還入力値が反転されるから、同じくクロック信号に基づいて 2^{17}-1 サイクルで循環的に変化するＭ系列１－２（図２（ｂ））が生成される。なお、Ｍ系列１－１とＭ系列１－２とは、変化のパターンは同一であるが、符号が互いに逆となっており、異なる疑似乱数系列として取り扱うことができる。これにより、切替部１６に与える切替信号が物理乱数で制御されるので、一方の疑似乱数系列を生成するシフトレジスタの途中情報を用いて、他方の疑似乱数系列から一方の疑似乱数系列に切り替えることにより、予測不可能な疑似乱数系列となる。また、二つの疑似乱数系列の「０」と「１」の頻度がそれぞれ 2^{16}-1 および 2^{16} と、2^{16} および 2^{16}-1 の対称比率になるので、二つの疑似乱数系列を物理乱数によって切り替え制御すれば、「０」と「１」の頻度分布状態が理想状態に近づくという効果もある。

図３に示すように、物理乱数発生器１４は、物理乱数発生源１４ａ、増幅回路１４ｂおよび二値化回路１４ｃを備える。このうち、物理乱数発生源１４ａは、自然現象に基づいてランダムに変化する信号を生じうるものであり、例えば、上記特許文献１に開示されるような、接合を含む電流路に生じる雑音信号を生じる半導体素子を含むものとすることができる。なお、これには限られず、放射性物質の崩壊を利用したもの等もこの物理乱数発生源１４ａとして用いることができる。物理乱数発生源１４ａにて生じた信号は、増幅回路１４ｂにおいて増幅され、さらに二値化回路１４ｃにおいて二値化処理される。二値化回路１４ｃは、所定のサンプリングタイミングで、増幅された信号の振幅と所定の閾値とを比較し、例えば、増幅された信号の振幅が所定の閾値より高いときには「１」を、逆に低

いときには「０」を出力する。こうして物理乱数発生器１４により、「１」または「０」を示す所定電圧の物理乱数出力値が生成される。なお、二値化回路１４ｃにおける閾値のレベルは任意に設定することができるが、通常は「１」および「０」の発生確率がほぼ１対１となるように設定される。なお、二値化回路１４ｃにおいて、単に、増幅された信号の振幅を所定の閾値と比較して出力信号を発生するようにしてもよい。

このように、本実施形態にかかる乱数発生装置１０では、二つの異なる疑似乱数系列のうちどちらを出力するかを、物理乱数によって切り替えるだけではなく、シフトレジスタの途中情報を有効に利用して二つの疑似乱数系列の帰還状態を変化させている。こうすることで、疑似乱数のみを用いた場合に比べて、乱数の予測が難しくなる。また、物理乱数を直接的な出力乱数としては用いないため、仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測性に対する影響は従来装置に比べてかなり小さくなる。

実施の形態２．　図４は本実施形態にかかる乱数生成装置３０の構成図である。乱数生成装置３０は、疑似乱数生成部３２、物理乱数発生器１４、および切替部３６を含む。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

本実施形態にかかる疑似乱数生成部３２では、線形シフトレジスタ符号発生器からの出力値を、切替部３６によって反転または非反転して出力乱数とする。図４の例では、シフトレジスタ１８およびＥＸＯＲゲート２０を含む典型的な線形シフトレジスタ符号発生器が構成されており、シフトレジスタ１８の所定ビット（例えば第１７番目のビット）のＱ出力およびＱｂ出力（Ｑ出力の反転出力）がそれぞれ切替部３６に入力される。

切替部３６は、二つのＡＮＤゲート３６ａ，３６ｂを備えており、そのうち一方のＡＮＤゲート３６ａには、Ｑｂ出力と物理乱数発生器１４からインバータ３６ｃを介して物理乱数出力が入力され、もう一方のＡＮＤゲート３６ｂには、Ｑ出力と物理乱数発生器１４からの物理乱数出力が入力される。そして、これら二つのＡＮＤゲート３６ａ，３６ｂの出力がＯＲゲート３６ｄに入力され、このＯＲゲート３６ｄの出力が出力乱数となる。

UTILITY/CIP APPLICATION CHECKLIST

Client/Matter Number: 04995/216001
Client/Matter Name: NGB / Hard Disk Recorder and Video Record Apparatus

---

IPDAS (Mandatory)

☐ ○	Transmittal – Utility Application	☐ ○	Application Cover Sheet	☐ ○	Application Data Sheet	☐ ○	Declaration
☐ ○	Postcard	☐ ○		☐ ○		☐ ○	

IPDAS (As Needed)

☐ ○	Fee Transmittal	☐ ○	Assignment	☐ ○	Assignment Recordation Coversheet	☐ ○	Preliminary Amendment
☐ ○	Information Disclosure Statement	☐ ○	Claim for Priority and Submission of Documents	☐ ○	Check Request/Credit Card Authorization Form	☐ ○	Non-Recordation Request
☐ ○	IDS Citation by Applicant	☐ ○		☐ ○		☐ ○	

APPLICATION FILE

☐○ If CIP, parent case is COMPLETE and PENDING. A Response to Missing Parts, and/or Petition for Extension has been filed. All outstanding rejections in the parent case have been answered

☐○ Cover sheet includes: title, names of ALL inventors, Express Mail stamp, and PTO Customer No. label.

☐○ Specification pages are present and checked for printer errors. Number of pages: _____

☐○ All figures are included and checked against the list of figures in the specification. Number of sheets: _____

☐○ At least one claim is included. Number of claims: _____ total / _____independent

☐○ Application has been reviewed to ensure all pages and figures are present. Claims have been reviewed by WA for obvious informalities.

☐○ Transmittal letter is complete and accurate, names ALL inventors, includes Express Mail stamp and PTO Customer No. label.

☐○ Declaration and Power of Attorney is signed/unsigned (circle one), and PTO Customer No. label is attached.

☐○ Check / Credit Card Authorization Form (circle one) for application fee is included. Amount: _____

☐○ If filed, an IDS letter and PTO Form SB-08 are complete and accurate, and PTO Customer No. label is attached. If an IDS is not filed with the application, a docketing entry has been entered for 3-months after filing date.

☐○ Original invention disclosure has been reviewed for additional prior art and other §102 events.

☐○ If filed, an assignment package contains a recordation cover sheet and all information is complete and accurate.

☐○ Express Mail Declarations include: correct Mailing Label Number and is addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

☐○ Postcard lists express mail number, all papers being sent and the number of pages of each.

△ WA has reviewed file, I-Manage, and e-mail to remove all work copies, notes and prior drafts.

△ If convention application, WA has reviewed claim for obvious informalities.

_____ _____
☐ Assistant ○ Double-checker

_____ Application filing package is substantively correct, complete, and complies with all client instructions.
△ (WA Initials)

_____ I have reviewed and approved the filing.
(AL Initials)

この切替部３６により、物理乱数出力に応じてＱ出力あるいはＱｂ出力のうちいずれか一方が有効となる。すなわち物理乱数出力値が「１」のときは、ＡＮＤゲート３６ａの出力値は必ず「０」となり、かつＡＮＤゲート３６ｂの出力値はＱｂ出力値と同じになるので、乱数出力値はＱｂ出力値と同じになる。逆に物理乱数出力値が「０」のときは、ＡＮＤゲート３６ｂの出力値は必ず「０」となり、かつＡＮＤゲート３６ａの出力値はＱ出力値と同じになるので、乱数出力値はＱ出力値と同じになる。すなわち、切替部３６の作用により、物理乱数出力値が「１」であるときは、Ｑ出力値を反転した値が出力乱数となり、逆に物理乱数出力が「０」であるときは、Ｑ出力値がそのまま出力乱数となっている。したがって、本実施形態にかかる乱数生成装置３０も、上記実施の形態１と同様に、図２に示した二つの乱数系列（Ｍ系列１－１，１－２）を、物理乱数によって切り替えて出力することができる。すなわち、このような構成によっても、上記実施の形態１と同様の効果が得られる。

実施の形態３．　図５は本実施形態にかかる乱数生成装置４０の構成図、また図６は、乱数生成装置４０によって生成される二つのＭ系列の巡回パターンを示す図である。乱数生成装置４０は、疑似乱数生成部４２、物理乱数発生器１４、および切替部４６を含む。なお、ここでも、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

本実施形態にかかる疑似乱数生成部４２では、線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく二種類の帰還入力値を生成することができる。そして、ＥＸＯＲゲート２０ｂの出力の通過／遮断を物理乱数によって決定している。具体的には、図５の例では、線形シフトレジスタ符号発生器として、シフトレジスタ１８と、異なるタップ出力の組み合わせについてそれぞれ排他的論理和を出力する複数のＥＸＯＲゲート２０ａ，２０ｂ，２０ｃとが設けられる。ＥＸＯＲゲート２０ａは、シフトレジスタ１８の入力側より第３番目と第１７番目のタップ出力（Ｑ３，Ｑ１７）の排他的論理和を出力し、ＥＸＯＲゲート２０ｂは、シフトレジスタ１８の入力側より第１番目と第２番目のタップ出力（Ｑ１，Ｑ２）の排他的論理和を出力する。ＥＸＯＲゲート２０ａの出力は直接ＥＸＯＲゲート２０ｃに入力されるが、ＥＸＯＲゲート２０ｂの出力はＡＮＤゲート（切

替部）４６を介してＥＸＯＲゲート２０ｃに入力される。ＡＮＤゲート４６には、物理乱数発生器１４からの物理乱数出力が入力される。

この構成では、物理乱数出力値が「１」である場合には、ＡＮＤゲート４６の出力値はＥＸＯＲゲート２０ｂの出力値と同じになるから、ＥＸＯＲゲート２０ｃからは、シフトレジスタ１８への帰還入力値として、ＥＸＯＲゲート２０ａの出力値とＥＸＯＲゲート２０ｂの出力値との排他的論理和が出力されることになる。他方、物理乱数出力値が「０」である場合には、ＡＮＤゲート４６の出力値は必ず「０」となるから、ＥＸＯＲゲート２０ｃからの出力値は、ＥＸＯＲゲート２０ａの出力値と同じになる。つまり、物理乱数出力値が「０」であるときはタップ出力（Ｑ３，Ｑ１７）に基づく帰還入力値が有効となるから、疑似乱数生成部１２においてM系列３－１（図６（ａ））が生成され、他方、物理乱数出力値が「１」であるときは、タップ出力（Ｑ１，Ｑ２，Ｑ３，Ｑ１７）に基づく帰還入力値が有効となるから、M系列３－２（図６（ｂ））が生成される。このように、本実施形態にかかる乱数生成装置４０も、二つの乱数系列（M系列３－１，３－２）を、物理乱数によって切り替えて出力することができる。

実施の形態４．　図７は本実施形態にかかる乱数生成装置５０の構成図、また図８は、乱数生成装置５０によって生成される三つのM系列の巡回パターンを示す図である。乱数生成装置５０は、疑似乱数生成部５２、物理乱数発生器１４、および切替部５６を含む。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

本実施形態にかかる疑似乱数生成部５２では、線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく三種類の帰還入力値を生成することができる。そして、それら三種類の帰還入力値のうちどれを有効とするかを、物理乱数によって決定している。具体的には、図７の例では、線形シフトレジスタ符号発生器として、シフトレジスタ１８と、異なるタップ出力の組み合わせに基づく入力値の排他的論理和を出力する複数のＥＸＯＲゲート２０ａ，２０ｂ，２０ｃ，２０ｄとが設けられる。ＥＸＯＲゲート２０ａは、シフトレジスタ１８の入力側より第３番目と第１７番目のタップ出力（Ｑ３，Ｑ１７）の排他的論理和を出力し、ＥＸＯＲゲート２０ｂは、シフトレジスタ１８の入力側より第１番目と第２

番目のタップ出力（Ｑ１，Ｑ２）の排他的論理和を出力し、またＥＸＯＲゲート２０ｃは、シフトレジスタ１８の入力側より第４番目と第７番目のタップ出力（Ｑ４，Ｑ７）の排他的論理和を出力する。ＥＸＯＲゲート２０ａの出力は直接ＥＸＯＲゲート２０ｄに入力されるが、ＥＸＯＲゲート２０ｂ，２０ｃの出力は、それぞれＡＮＤゲート５６ｂ，５６ｃおよびＯＲゲート５６ｄを介してＥＸＯＲゲート２０ｄに入力される。またＡＮＤゲート５６ｂ，５６ｃには、三分周器５６ａからの出力が入力される。

本実施形態では、三分周器５６ａ、ＡＮＤゲート５６ｂ，５６ｃおよびＯＲゲート５６ｄが、切替部５６として機能する。この構成において、公知の構成を有する三分周器５６ａは、物理乱数発生器１４からの物理乱数出力をクロックとして、そのＱ１出力値およびＱ２出力値を、「０」,「０」（パターン１）、「０」,「１」（パターン２）、「１」,「０」（パターン３）の三パターンで巡回的に更新する。そしてパターン１、すなわちＱ１出力値：「０」、Ｑ２出力値：「０」のときは、ＯＲゲート５６ｄの出力値は「０」となり、この場合には、ＥＸＯＲゲート２０ａの出力値が、シフトレジスタ１８に帰還入力値として入力される。同様にパターン２、すなわちＱ１出力値：「１」、Ｑ２出力値：「０」のときは、ＯＲゲート５６ｄの出力値は、ＥＸＯＲゲート２０ｂの出力値と同じになる。したがってこの場合には、ＥＸＯＲゲート２０ｄからは、シフトレジスタ１８への帰還入力値として、ＥＸＯＲゲート２０ａの出力値とＥＸＯＲゲート２０ｂの出力値との排他的論理和が出力される。またパターン３、すなわちＱ１出力値「１」，Ｑ２出力値：「０」のときは、ＯＲゲート５６ｄの出力値は、ＥＸＯＲゲート２０ｃの出力と同じ値となる。したがってこの場合には、ＥＸＯＲゲート２０ｄからは、シフトレジスタ１８への帰還入力値として、ＥＸＯＲゲート２０ａの出力値とＥＸＯＲゲート２０ｃの出力値との排他的論理和が出力される。つまり、物理乱数出力が更新されるたびに、疑似乱数生成部１２において、［１］ＥＸＯＲゲート２０ａに入力されるタップ出力（Ｑ３，Ｑ１７）に基づく帰還入力値が有効となるＭ系列４－１（図８（ａ））、［２］ＥＸＯＲゲート２０ａ，２０ｂに入力されるタップ出力（Ｑ１，Ｑ２，Ｑ３，Ｑ１７）に基づく帰還入力値が有効となるＭ系列４－２（図８（ｂ））、および［３］ＥＸＯＲゲート２０ａ，２０ｃに入力されるタップ出力（Ｑ

３，Ｑ４，Ｑ７，Ｑ１７）に基づく帰還入力値が有効となるM系列４－３（図８（ｃ））が生成される。このように、本実施形態にかかる乱数生成装置５０は、三つの乱数系列（M系列４－１，４－２，４－３）を、物理乱数によって切り替えて出力することができる。

実施の形態５．　図９は本実施形態にかかる乱数生成装置６０の構成図、また図１０は、乱数生成装置６０によって生成される二つのM系列の巡回パターンを示す図である。乱数生成装置６０は、疑似乱数生成部６２、物理乱数発生器１４、および切替部６６を含む。なお、ここでも、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

本実施形態にかかる疑似乱数生成部６２は、帰還入力を得るタップ（帰還入力の元となるタップ）は同一とし、シフトレジスタのビット数を変更するように構成されており、該シフトレジスタのビット数の変更を物理乱数によって決定している。具体的には、図９の例では、線形シフトレジスタ符号発生器として、１５段のシフトレジスタ６８と、縦続に配置された二つのフリップフロップ６２ａ，６２ｂと、所定のタップ出力の組み合わせについて排他的論理和を出力するＥＸＯＲゲート２０ｅとが設けられる。ＥＸＯＲゲート２０ｅは、シフトレジスタ６８の入力側より第１番目と第１５番目のタップ出力（Ｑ１，Ｑ１５）の排他的論理和を出力する。ＥＸＯＲゲート２０ｅの出力は、前段側のフリップフロップ６２ａと、ＡＮＤゲート６６ａとに入力される。

切替部６６は、二つのＡＮＤゲート６６ａ，６６ｂを備えており、そのうち一方のＡＮＤゲート６６ａには、ＥＸＯＲゲート２０ｅの出力と物理乱数発生器１４からの物理乱数出力が入力され、もう一方のＡＮＤゲート６６ｂには、Ｑ出力と物理乱数発生器１４からインバータ６６ｃを介して物理乱数出力が入力される。そして、これら二つのＡＮＤゲート６６ａ，６６ｂの出力がＯＲゲート６６ｄに入力され、このＯＲゲート６６ｄの出力がシフトレジスタ６８に入力される。

この切替部６６により、物理乱数出力に応じて、ＥＸＯＲゲート２０ｅの出力あるいはフリップフロップ６２ｂの出力のうちいずれか一方が有効となる。すなわち物理乱数出力値が「０」のときは、ＡＮＤゲート６６ａの出力値は必ず「０」となり、かつＡＮＤゲート６６ｂの出力値はフリップフロップ６２ｂの出力値と

同じになるから、ＯＲゲート６６ｄの出力値はフリップフロップ６２ｂの出力値と同じになる。逆に物理乱数出力値が「１」のときは、ＡＮＤゲート６６ｂの出力は必ず「０」となり、かつＡＮＤゲート６６ａの出力値はＥＸＯＲゲート２０ｅの出力値と同じになるから、ＯＲゲート６６ｄの出力値はＥＸＯＲゲート２０ｅの出力値と同じ値となる。すなわち、切替部６６の作用により、物理乱数出力値が「０」であるときは、フリップフロップ６２ａ，６２ｂもシフトレジスタの一部として機能することになり、これらを含めた１７段のシフトレジスタによって、タップ出力（Ｑ３，Ｑ１７）に基づく帰還入力値が有効となるＭ系列５－１（図１０（ａ））が生成される。他方、物理乱数出力が「１」であるときは、フリップフロップ６２ａ，６２ｂは無効となり、１５段のシフトレジスタ６８によって、タップ出力（Ｑ１，Ｑ１５）に基づく帰還入力値が有効となるＭ系列５－２（図１０（ｂ））が生成される。このように、本実施形態にかかる乱数発生装置６０は、段数の異なる二つのシフトレジスタによって発生される乱数系列（Ｍ系列５－１，５－２）を、物理乱数によって切り替えて出力することができる。

実施の形態６．　図１１は本実施形態にかかる乱数生成装置７０の構成図である。乱数生成装置７０は、疑似乱数生成部７２、物理乱数発生器１４、および切替部１６を含む。本実施形態の疑似乱数生成部７２は、シフトレジスタ７８（１８）内に後述する検出回路７８ａが設けられている点を除いては実施の形態１の疑似乱数生成部１２と同じであり、図２に示すＭ系列１－１，１－２を生成することができる。なお、ここでも、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

線形シフトレジスタ符号発生器は、シフトレジスタ内の符号列によっては、Ｍ系列符号を生成できない。例えば、シフトレジスタの全ビットの値が「０」である場合にはＭ系列１－１を生成することができないし、また、シフトレジスタの全ビットが「１」である場合にはＭ系列１－２を生成することができない。一の疑似乱数系列の符号のみを生成する従来の一般的な線形シフトレジスタ符号発生器では、例えば初期値をそのような符号列としないように留意すれば十分であったが、上記実施形態のように、生成される疑似乱数系列が動作中に変更される場合には、有効な疑似乱数系列に対してシフトレジスタ内の符号列が該系列を生じ

ないものとならないようにするための対策を講じておくのが望ましい。そのために、本実施形態にかかる乱数生成装置７０は、上記実施の形態１にかかる乱数生成装置１０に、検出回路７８ａ，７８ｂ、ＡＮＤゲート８２ａ，８２ｂ、フリップフロップ８４ａ，８４ｂ、およびフリップフロップ８０を付加した構成となっている。

上記付加的な構成要素について説明する。物理乱数発生器１４からの出力（物理乱数出力）は、フリップフロップ８０に入力される。なお、本実施形態でも、物理乱数出力値「０」はM系列１－１（図２（ａ））を、また「１」はM系列１－２（図２（ａ））を示すものとして規定されている。検出回路７８ａは、シフトレジスタ７８の全ビットの値が「１」であるときに、ＡＮＤゲート８２ａに「１」を出力する（例えば全ビットの値の論理積を出力する）。また検出回路７８ｂは、シフトレジスタ７８の全ビットの値が「０」であるときに、ＡＮＤゲート８２ｂに「１」を出力する（例えば全ビットの反転値の論理積を出力する）。ＡＮＤゲート８２ａには、検出回路７８ａの出力とフリップフロップ８０のＱ出力とが入力され、その出力はフリップフロップ８４ａに入力される。ＡＮＤゲート８２ｂには、検出回路７８ｂの出力とフリップフロップ８０のＱｂ出力とが入力され、その出力はフリップフロップ８４ｂに入力される。そして、フリップフロップ８４ａの出力はリセット信号（Ｒ入力）として、またフリップフロップ８４ｂの出力はセット信号（Ｓ入力）として、フリップフロップ８０に入力される。なお、図１１の例では、検出回路７８ａ，７８ｂはシフトレジスタ７８に内蔵されているが、これらをシフトレジスタ７８の外部に接続してもよい。

上記構成において、シフトレジスタ７８の全ビットの値が「１」であるときに、物理乱数出力値が「０」から「１」に変化すると、フリップフロップ８０の値は「１」となり、Ｑ出力値が「１」となる。また、検出回路７８ａの出力値は「１」であるから、ＡＮＤゲート８２ａの出力値は「１」となる。そして、フリップフロップ８４ａの値が「１」となって、フリップフロップ８０にリセット信号が入力される。したがって、この場合、フリップフロップ８０の値は「１」から「０」に変更される。すなわち上記構成によれば、シフトレジスタ７８においてM系列１－１（図２（ａ））の符号が生じない状態（すなわち全ビットの値が「０」）と

なるのを防止することができる。

一方、シフトレジスタ７８の全ビットの値が「０」であるときに、物理乱数出力値が「１」から「０」に変化すると、フリップフロップ８０の値が「０」となり、Ｑｂ出力値が「１」となる。また、検出回路７８ｂの出力値は「１」であるから、ＡＮＤゲート８２ｂの出力値は「１」となる。そして、フリップフロップ８４ｂの値が「１」となって、フリップフロップ８０にセット信号が入力される。したがって、この場合、フリップフロップ８０の値は「０」から「１」に変更される。すなわち上記構成によれば、シフトレジスタ７８においてM系列１－２（図２（ｂ））の符号が生じない状態（すなわち全ビットの値が「１」）となるのを防止することができる。

なお、フリップフロップ８４ａ，８４ｂの出力により、シフトレジスタ７８の少なくとも一つのビットの値を変化させるようにしても同様の効果が得られる。例えば、フリップフロップ８４ａの出力を、シフトレジスタ７８内を構成する少なくとも一つのフリップフロップのリセット信号とすれば、当該フリップフロップ（ビット）の値が「０」となるので、M系列１－１の符号を生じない状態となるのを防止することができる。また、フリップフロップ８４ｂの出力をシフトレジスタ７８内を構成するいずれかのフリップフロップのリセット信号とすれば、当該フリップフロップ（ビット）の値が「１」となるので、M系列１－２の符号を生じない状態となるのを防止することができる。

以上、本発明の好適な実施形態について説明したが、本発明は上記実施形態で示した構成には限定されず、種々の等価回路によっても実施可能である。上記実施形態では、疑似乱数が、１７段または１５段のシフトレジスタを有する線形シフトレジスタ符号発生器によって生成される数種類のM系列符号である場合を例示したが、これには限定されず、それ以外の段数のシフトレジスタあるいはタップの組み合わせに基づくM系列であってもよい。また、上記実施の形態６は、上記実施の形態１を基礎としたものを例示的に示したが、他の実施形態に対しても同様に適用可能であることは言うまでもない。また、上記実施の形態１，３～６では、シフトレジスタの最終段のフリップフロップからの出力を乱数出力としたが、他のフリップフロップからの出力を乱数出力としてもよいし、シフトレジス

タに入力される帰還値を乱数出力としてもよい。

産業上の利用可能性

以上説明したように、本発明によれば、複数の疑似乱数系列のうちどれを有効とするかを物理乱数によって切り替えるため、その予測が難しく暗号化アルゴリズム等への適用に際してより安全性の高い乱数を生成することができる。このため、例えば、より高い安全性が要求される暗号化技術等での使用に適している。

請 求 の 範 囲

１.複数の異なる疑似乱数系列の乱数パターンを出力可能な疑似乱数生成手段と、
物理乱数を生成する物理乱数生成手段と、
前記物理乱数生成手段の生成した物理乱数に基づいて前記疑似乱数生成手段の出力する乱数の疑似乱数系列を切り替える切替手段と、
を備える乱数生成装置。

２．前記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、
前記切替手段は、前記線形シフトレジスタ符号発生器への帰還入力値の反転／非反転を、前記物理乱数生成手段によって生成された物理乱数に基づいて切り替えることを特徴とする請求の範囲第１項に記載の乱数生成装置。

３．前記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、
前記切替手段は、前記線形シフトレジスタ符号発生器からの出力値の反転／非反転を、前記物理乱数生成手段によって生成された物理乱数に基づいて切り替えることを特徴とする請求の範囲第１項に記載の乱数生成装置。

４．前記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、該線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく複数の帰還入力値を生成し、
前記切替手段は、前記生成された複数の帰還入力値のうち該線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、前記物理乱数生成手段で生成された物理乱数に基づいて切り替えることを特徴とする請求の範囲第１項に記載の乱数生成装置。

５．前記疑似乱数生成手段は、所定のタップの組み合わせに基づく第一の帰還入力値を生成する線形シフトレジスタ符号発生器と、該第一の帰還入力値を受け取り前記線形シフトレジスタ符号発生器と同期して所定ビット数ビットシフトを行いその出力を第二の帰還入力値とするフリップフロップと、を含み、

前記切替手段は、前記第一または第二の帰還入力値のうち前記線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、前記物理乱数生成手段で生成された物理乱数に基づいて切り替えることを特徴とする請求の範囲第１項に記載の乱数生成装置。

６．請求の範囲第２項に記載の乱数生成装置であって、

前記線形シフトレジスタ符号発生器の符号列を検出する検出手段を備え、

前記切替手段は、有効な疑似乱数系列の乱数が前記検出された符号列によっては生成不能である場合には、該疑似乱数系列以外の疑似乱数系列に切り替えることを特徴とする乱数生成装置。

７．請求の範囲第２項に記載の乱数生成装置であって、

前記線形シフトレジスタ符号発生器の符号列を検出する検出手段と、

有効な疑似乱数系列の乱数が前記検出された符号列によっては生成不能である場合には、前記符号列のビット値のうち少なくとも一つを反転させることを特徴とする乱数生成装置。

図1

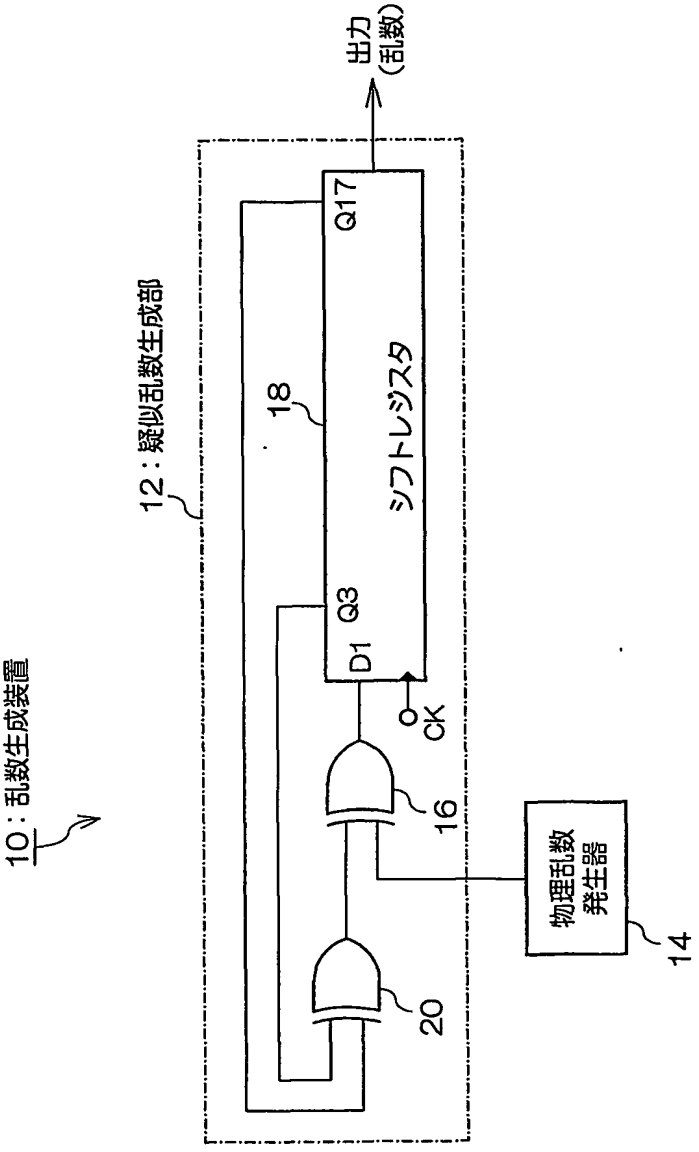

出力
(乱数)
Q17
12：疑似乱数生成部
18
シフトレジスタ
Q3
D1
CK
16
物理乱数
発生器
14
20
10：乱数生成装置

図2

(a)

M系列1-1 (物理乱数：0)	FF 1	2	3	4	5	・・・	16	17
タイミング t(1)	1	1	1	1	1	・・・	1	1
t(2)	0	1	1	1	1	・・・	1	1
t(3)	0	0	1	1	1	・・・	1	1
t(4)	0	0	0	1	1	・・・	1	1
t(5)	1	0	0	0	1	・・・	1	1
t(6)	1	1	0	0	0	・・・	1	1
⋮			⋮				⋮	
$t(2^{17}-1)$	1	1	1	1	1	・・・	1	0

(b)

M系列1-2 (物理乱数：1)	FF 1	2	3	4	5	・・・	16	17
タイミング t(1)	0	0	0	0	0	・・・	0	0
t(2)	1	0	0	0	0	・・・	0	0
t(3)	1	1	0	0	0	・・・	0	0
t(4)	1	1	1	0	0	・・・	0	0
t(5)	0	1	1	1	0	・・・	0	0
t(6)	0	0	1	1	1	・・・	0	0
⋮			⋮				⋮	
$t(2^{17}-1)$	0	0	0	0	0	・・・	0	1

図3

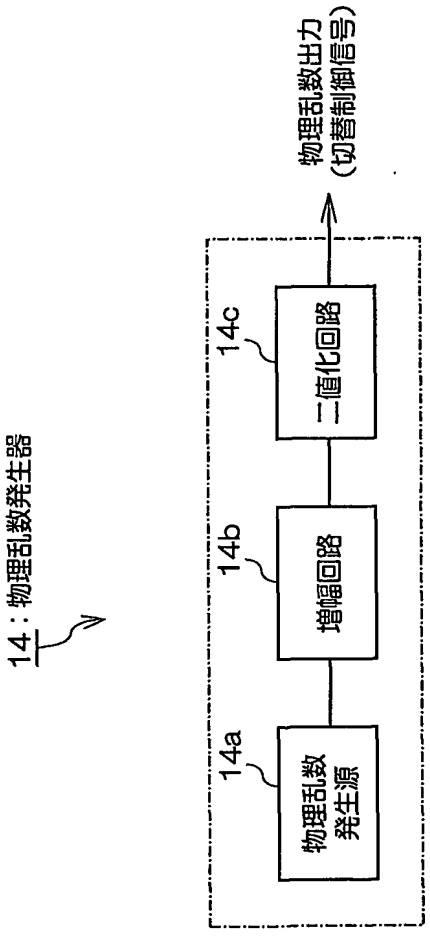


図4

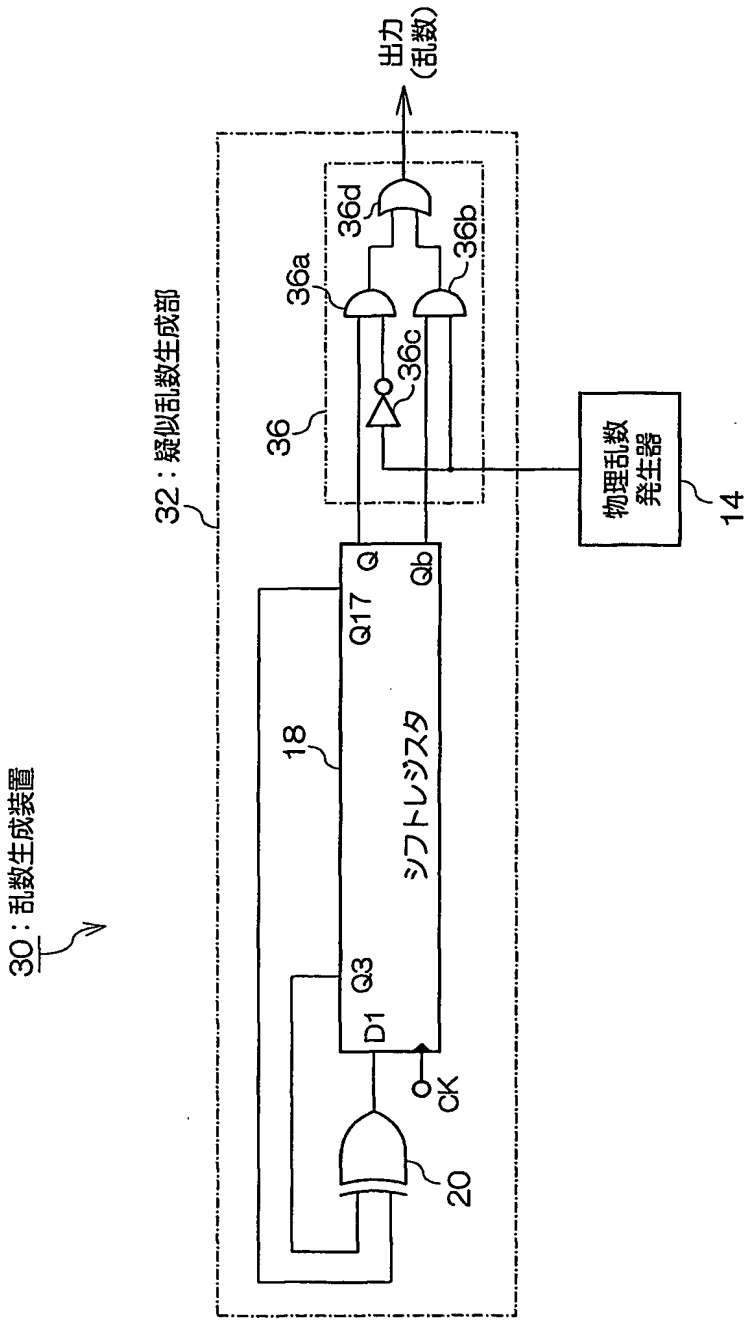

出力
(乱数)
32：疑似乱数生成部
36d
36a
36b
36c
36
物理乱数
発生器
14
Q
Qb
Q17
18
シフトレジスタ
Q3
D1
CK
20
30：乱数生成装置

図5

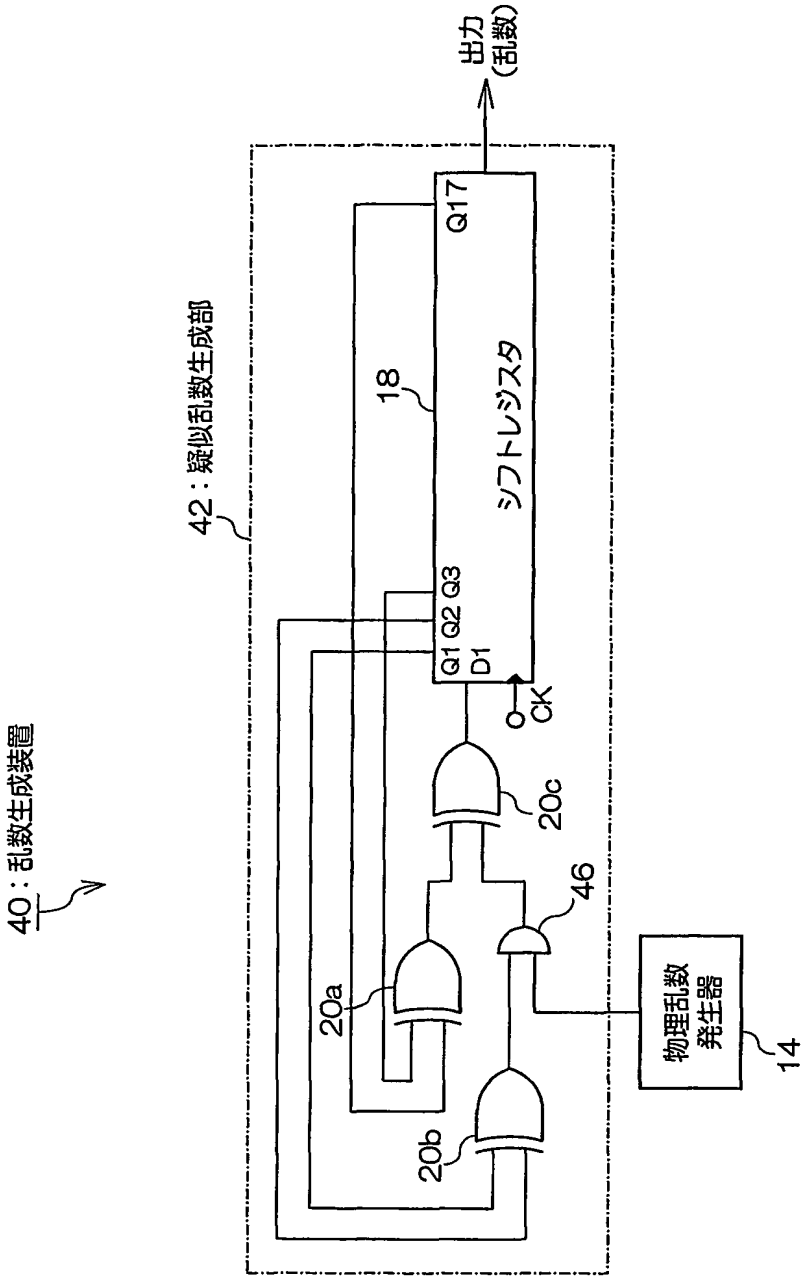

出力
(乱数)
42：疑似乱数生成部
Q17
18
シフトレジスタ
Q1 Q2 Q3
D1
CK
20c
46
20a
20b
物理乱数
発生器
14
40：乱数生成装置

図6

(a)

M系列3-1 (物理乱数：0)	FF 1	2	3	4	5	・・・	16	17
タイミング t(1)	1	1	1	1	1	・・・	1	1
t(2)	0	1	1	1	1	・・・	1	1
t(3)	0	0	1	1	1	・・・	1	1
t(4)	0	0	0	1	1	・・・	1	1
t(5)	1	0	0	0	1	・・・	1	1
t(6)	1	1	0	0	0	・・・	1	1
⋮			⋮				⋮	
$t(2^{17}-1)$	1	1	1	1	1	・・・	1	0

⇕

(b)

M系列3-2 (物理乱数：1)	FF 1	2	3	4	5	・・・	16	17
タイミング t(1)	1	1	1	1	1	・・・	1	1
t(2)	0	1	1	1	1	・・・	1	1
t(3)	1	0	1	1	1	・・・	1	1
t(4)	0	1	0	1	1	・・・	1	1
t(5)	0	0	1	0	1	・・・	1	1
t(6)	1	0	0	1	0	・・・	1	1
⋮			⋮				⋮	
$t(2^{17}-1)$	1	1	1	1	1	・・・	1	0

図7

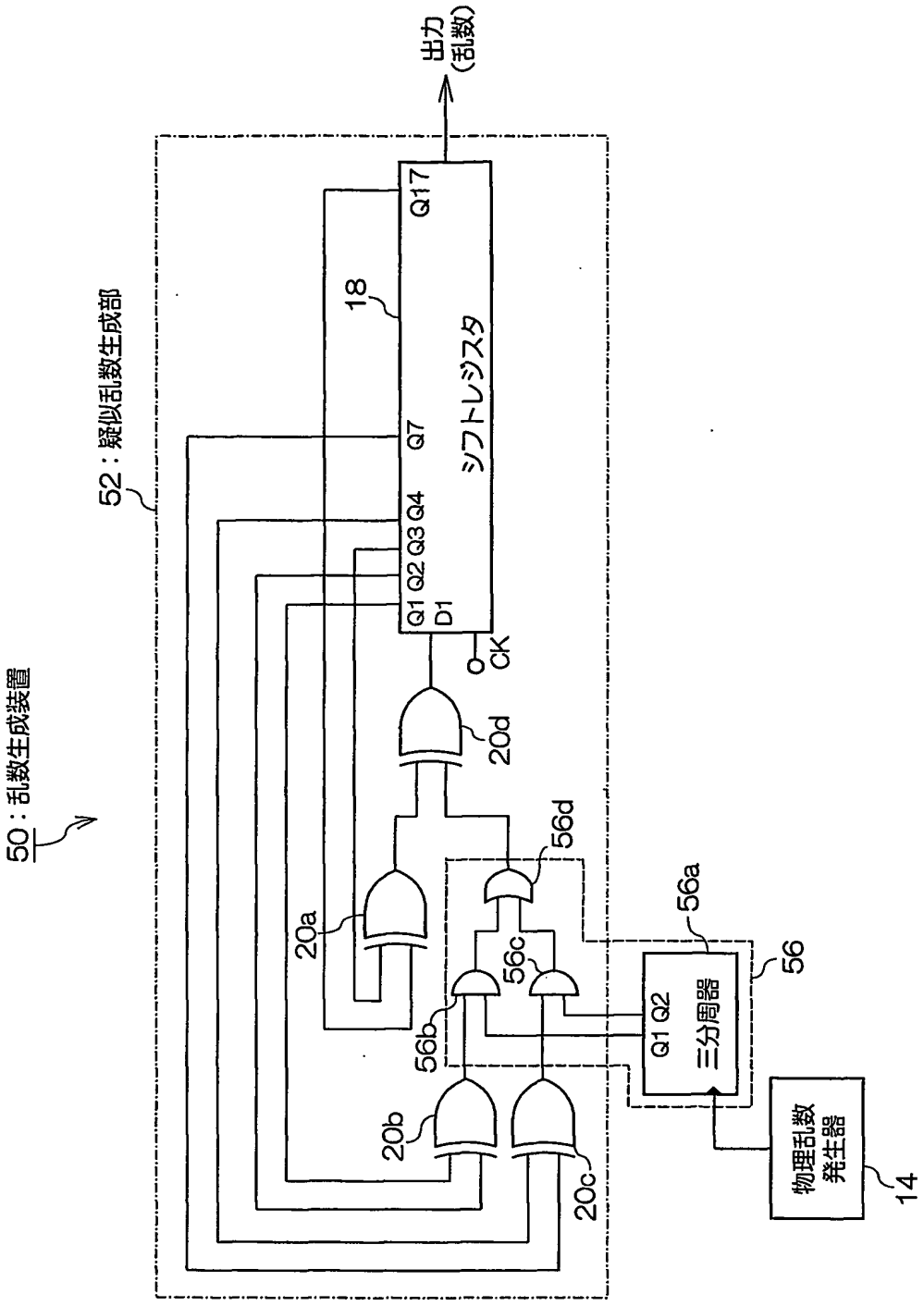

出力
(乱数)
52：疑似乱数生成部
50：乱数生成装置
18
シフトレジスタ
Q17
Q7
Q4
Q3
Q2
Q1
D1
CK
20a
20b
20c
20d
56
56a
56b
56c
56d
三分周器
Q1 Q2
物理乱数
発生器
14

図8

(a)

M系列4-1 (Q1=0,Q2=0)

タイミング	FF 1	2	3	4	5	・・・	16	17
t(1)	1	1	1	1	1	・・・	1	1
t(2)	0	1	1	1	1	・・・	1	1
t(3)	0	0	1	1	1	・・・	1	1
t(4)	0	0	0	1	1	・・・	1	1
t(5)	1	0	0	0	1	・・・	1	1
t(6)	1	1	0	0	0	・・・	1	1
：			：				：	
$t(2^{17}-1)$	1	1	1	1	1	・・・	1	0

(b)

M系列4-2 (Q1=1,Q2=0)

タイミング	FF 1	2	3	4	5	・・・	16	17
t(1)	1	1	1	1	1	・・・	1	1
t(2)	0	1	1	1	1	・・・	1	1
t(3)	1	0	1	1	1	・・・	1	1
t(4)	0	1	0	1	1	・・・	1	1
t(5)	0	0	1	0	1	・・・	1	1
t(6)	0	0	0	1	0	・・・	1	1
：			：				：	
$t(2^{17}-1)$	1	1	1	1	1	・・・	1	0

(c)

M系列4-3 (Q1=0,Q2=1)

タイミング	FF 1	2	3	4	5	・・・	16	17
t(1)	1	1	1	1	1	・・・	1	1
t(2)	0	1	1	1	1	・・・	1	1
t(3)	0	0	1	1	1	・・・	1	1
t(4)	0	0	0	1	1	・・・	1	1
t(5)	1	0	0	0	1	・・・	1	1
t(6)	0	1	0	0	0	・・・	1	1
：			：				：	
$t(2^{17}-1)$	1	1	1	1	1	・・・	1	0

図9

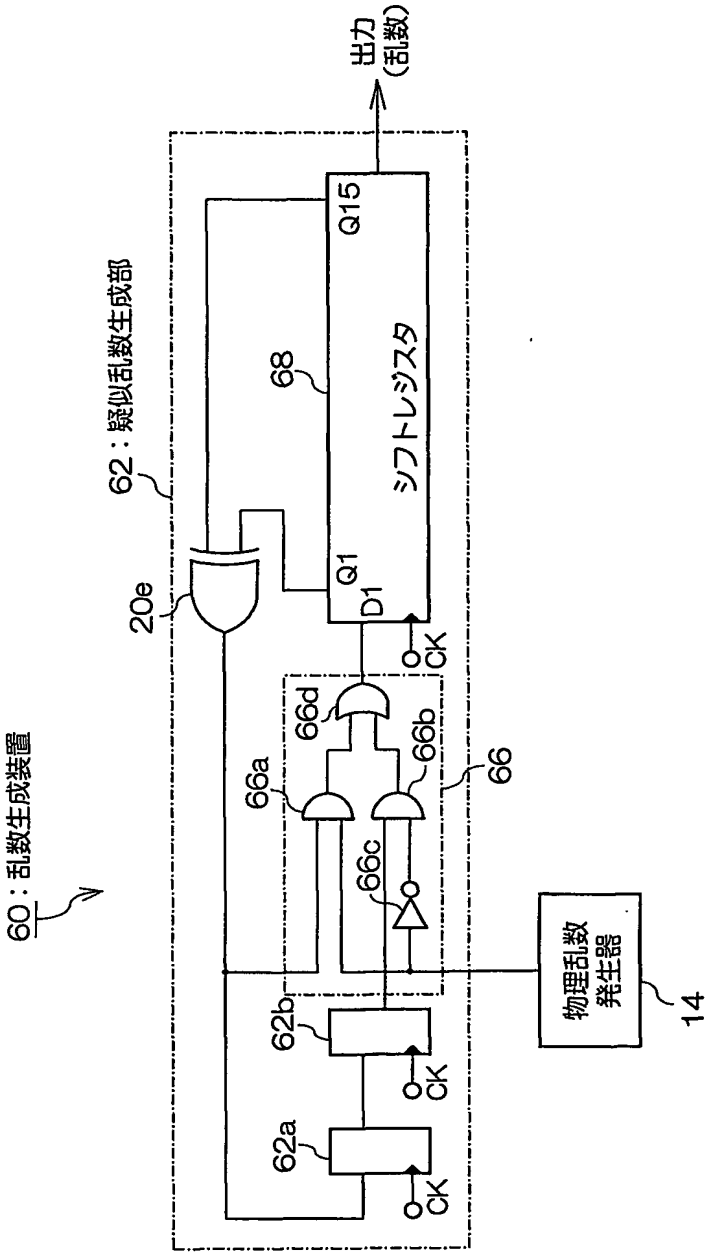

出力
(乱数)
62：疑似乱数生成部
60：乱数生成装置
68
シフトレジスタ
Q15
Q1
D1
CK
20e
66d
66b
66a
66c
66
62b
62a
物理乱数
発生器
14

図10

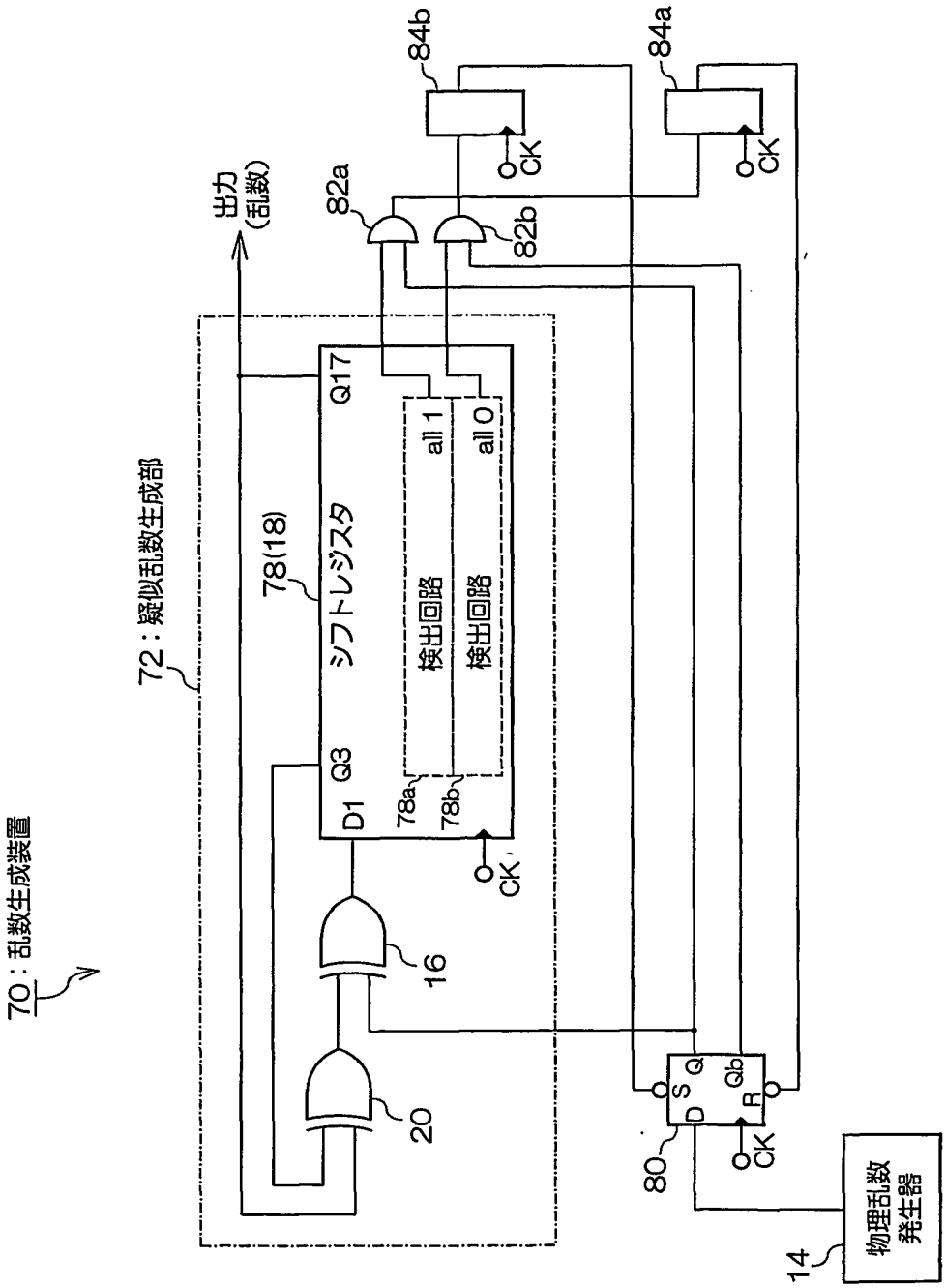
(a)

M系列5-1 (物理乱数:0)	FF 1	2	3	4	5	・・・	16	17
タイミング t(1)	1	1	1	1	1	・・・	1	1
t(2)	0	1	1	1	1	・・・	1	1
t(3)	0	0	1	1	1	・・・	1	1
t(4)	0	0	0	1	1	・・・	1	1
t(5)	1	0	0	0	1	・・・	1	1
t(6)	1	1	0	0	0	・・・	1	1
⋮			⋮				⋮	
$t(2^{17}-1)$	1	1	1	1	1	・・・	1	0

(b)

M系列5-2 (物理乱数:1)	FF 1	2	3	4	5	・・・	14	15
タイミング t(1)	1	1	1	1	1	・・・	1	1
t(2)	0	1	1	1	1	・・・	1	1
t(3)	1	0	1	1	1	・・・	1	1
t(4)	0	1	0	1	1	・・・	1	1
t(5)	1	0	1	0	1	・・・	1	1
t(6)	1	1	0	1	0	・・・	1	1
⋮			⋮				⋮	
$t(2^{17}-1)$	1	1	1	1	1	・・・	1	0

図11


70：乱数生成装置
72：疑似乱数生成部
78(18)
シフトレジスタ
Q17
Q3
D1
all 1
all 0
検出回路
検出回路
78a
78b
CK'
16
20
出力
(乱数)
82a
82b
84b
84a
CK
S
R
Q
Qb
D
80
物理乱数
発生器
14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/14055

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/24, G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/24, G06F7/58

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Microfilm of the specification and drawings annexed to the request of Japanese Utility Model Application No. 54192/1980(Laid-open No. 156134/1981) (Nikoo-Electronics Co., Ltd.), 21 November, 1981 (21.11.81), Full text; Figs. 1 to 2 (Family: none)	1-7
Y	JP 10-262041 A (International Business Machines Corp.), 29 September, 1998 (29.09.98), Par. No. [0018]; Fig. 1 & US 6282291 B	1-7

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 February, 2004 (03.02.04)	17 February, 2004 (17.02.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/14055

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 8-503569 A (Motorola, Inc.), 16 April, 1996 (16.04.96), Page 11, line 28 to page 13, line 20; Fig. 2 & DE 69429157 D & US 5365585 A & CA 2146439 A & WO 95/06906 A & FI 951946 A & GB 2286274 A & HK 1002338 A & KR 168504 B & BR 9405567 A & SG 76452 A & EP 672273 A & DE 69429157 T	2,4-7
Y	JP 9-509748 A (RAIKE, William, Michael), 30 September, 1997 (30.09.97), Page 28, line 25 to page 30, line 22; Fig. 1 & AU 1204995 A & AU 1132199 A & WO 95/15633 A & EP 734624 A & NZ 277128 A & US 5799088 A & NZ 329808 A & NZ 336413 A & NZ 336414 A & AU 729638 B & JP 2002-314534 A & JP 3339688 B	3

国際[redacted]報告

国際出願番[redacted]PCT／JP03／14055

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／24　G06F7／58

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／24　G06F7／58

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	日本国実用新案登録出願55－54192号（日本国実用新案登録出願公開56－156134号）の願書に添付した明細書及び図面の内容を記録したマイクロフィルム（ニコー電子株式会社） 1981．11．21，全文，第1－2図（ファミリーなし）	1－7
Y	JP　10－262041　A（インターナショナル・ビジネス・マシーンズ・コーポレイション） 1998．09．29，第【0018】段落，図1 ＆　US　6282291　B	1－7

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 03．02．2004	国際調査報告の発送日　17. 2. 2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5M　4229 青木　重徳 電話番号　03－3581－1101　内線　3597

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP　8－503569　A（モトローラ・インコーポレイテッド） 1996．04．16 第11頁第28行－第13頁第20行，図2 & DE 69429157 D & US 5365585 A & CA 2146439 A & WO 95／06906 A & FI 951946 A & GB 2286274 A & HK 1002338 A & KR 168504 B & BR 9405567 A & SG 76452 A & EP 672273 A & DE 69429157 T	2，4－7
Y	JP　9－509748　A（ライク，ウイリアム，マイケル） 1997．09．30 第28頁第25行－第30頁第22行，FIG．1 & AU 1204995 A & AU 1132199 A & WO 95／15633 A & EP 734624 A & NZ 277128 A & US 5799088 A & NZ 329808 A & NZ 336413 A & NZ 336414 A & AU 729638 B & JP 2002－314534 A & JP 3339688 B	3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/14055

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/24, G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/24, G06F7/58

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Microfilm of the specification and drawings annexed to the request of Japanese Utility Model Application No. 54192/1980(Laid-open No. 156134/1981) (Nikoo-Electronics Co., Ltd.), 21 November, 1981 (21.11.81), Full text; Figs. 1 to 2 (Family: none)	1-7
Y	JP 10-262041 A (International Business Machines Corp.), 29 September, 1998 (29.09.98), Par. No. [0018]; Fig. 1 & US 6282291 B	1-7

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 03 February, 2004 (03.02.04)	Date of mailing of the international search report 17 February, 2004 (17.02.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/14055

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 8-503569 A (Motorola, Inc.), 16 April, 1996 (16.04.96), Page 11, line 28 to page 13, line 20; Fig. 2 & DE 69429157 D & US 5365585 A & CA 2146439 A & WO 95/06906 A & FI 951946 A & GB 2286274 A & HK 1002338 A & KR 168504 B & BR 9405567 A & SG 76452 A & EP 672273 A & DE 69429157 T	2,4-7
Y	JP 9-509748 A (RAIKE, William, Michael), 30 September, 1997 (30.09.97), Page 28, line 25 to page 30, line 22; Fig. 1 & AU 1204995 A & AU 1132199 A & WO 95/15633 A & EP 734624 A & NZ 277128 A & US 5799088 A & NZ 329808 A & NZ 336413 A & NZ 336414 A & AU 729638 B & JP 2002-314534 A & JP 3339688 B	3